5-22-09

Chris.Gunderson@w2cog.org

MEMORANDUM FOR THE RECORD

Ref: (a) CJCSM 3170.01C. Operation of the Joint Capabilities Integration and Development System, 1 May 2007

(b) DODD 4630.5 Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), 5 May 2004

(c) DoDI 4630.8. Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), 30 June 2004

(d) CJCSI 6212.01 Interoperability and Supportability of Informatioin Technology and National Security Systems, 15 Dec 2008.

(e) Defense Science Board (DSB) Report on DoD Policy and Procedures for Acquisition of Information Technology, Mar 2009

Subj: NET-READY KEY PERFORMANCE PARAMETER (NR-KPP) AS A PRAGMATIC VALUE METRIC

1. Enclosure (b) to reference (a) explains Chairman Joint Chief of Staff (CJCS) policy for Key Performance Parameters (KPP). References (b) and (c) provide Office of the Secretary of Defense (OSD) policy and implementation guidance, respectively, for interoperability and sustainability of DoD Information Technology (IT) and National Security Systems (NSS). References (b) and (c) established the Net Ready Key Performance Parameter (NR-KPP) to "assess net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange." Reference (d) is the CJCS implementation guidance for the NR-KPP.

2. Per reference (a), a Key Performance Parameter (KPP) is a formally designated requirement specification for DoD systems. KPPs are objective metrics with stated values for threshold (minimum acceptable) and objective (desired) values. KPPs should:

a. Address something that is "key", i.e., important;

b. Address "performance", i.e. useful outcomes;

c. Be testable, i.e. objective, and measurable, predictable, and/or calculable. In other words the "P" for "Parameter" in KPP is in the mathematical sense.

3. "Sustainability" targets like "reliability = 0.99999", and "Survivability" targets like "maximum speed no less than mach 2.0" are examples of traditional KPPs that have the qualities described in paragraph 2.

4. Some KPPs are mandatory: for example the "Sustainability" "Material Availability" KPP. Material Availability KPPs are often formulated as "Operational Availability" (A_o). $A_{o,}$ is

calculated by dividing system “up time” by “up time” plus “down time.” A_o is a particularly good KPP because it not only measures a critical operational parameter, system reliability, but it can be formulated with metrics that point to options for achieving objective and threshold targets. The A_o component metrics are typically Mean Time Between Failure (MTBF), Mean Logistics Delay Time (MLDT), and Mean Time to Repair (MTTR) such that Ao = MTBF/(MTBF + MLDT + MTTR)

5. Any or all of MTBF, MLDT, or MTTR could be designated as KPPs in their own right. Each addresses important, objective, performance outcomes. However, most often they are treated as components of the composite metric $A_{o.}$ This is because such holistic treatment gives programs a clearer view of the trade space available to achieve their thresholds and objectives. For example building in redundant capability to increase MTBF, provisioning on-site spares to reduce MLDT, and maintaining on-site technicians to decrease MTTR, are all options that can improve over all Operational Availability.

6. The NR-KPP is also mandatory. Per references (a)-(d), NR-KPP should specify objective threshold targets for technical exchange of information and the operational effectiveness of that exchange. Metrics for technical exchange performance might be, for example, “transactional latency” or “transactional vulnerability.” Metrics for operational effectiveness might be, for example, “Probability of Fratricide” (PF) or “Probability of Kill” (PK).

7. Arguably, complying with “open” standards is a necessary condition for achieving pragmatic, cost effective, and widespread interoperability and supportability. However, defining mandatory universal standards, and defining “compliance” universally, has historically been ineffective for achieving universal interoperability and supportability.

8. Hence, while demonstrated “compliance” with a particular standard might be an important metric, demonstrating such compliance in and of itself cannot be considered a KPP. Measured compliance with standards is at best a predictor of performance. Reference (a) describes KPPs as metrics of demonstrated performance.

9. Rather, programs should select the most up to date applicable standards, and the associated implementation choices, based on their performance targets. In other words, choices of the standards and implementation methods are among the options that allow a program to achieve its KPP target. In the A_o example in paragraph 5, choice of, e.g., either LINUX or WINDOWS operating systems, will impact MTBF, MLDT, and MTTR and associated costs.

10. In the NR-KPP example (paragraph 6) the operational efficiency targets will provide the basis for determining the technical exchange performance targets. For example, stringent PF requirements might drive requirements for highly assured transactional authentication and authorization. On the other hand, PK requirements may or may not drive stringent transactional latency requirements. It will depend on the details of the mission threads of interest. The evolving stat- of-the-art of existing commercial standards for things like communications protocols, service discovery, real time publish-subscribe solutions, security, etc. will define the engineering options and trade offs.

11. KPPs are not necessarily independent of each other. Reference (a) explains that programs will typically improve iteratively from its KPP threshold to its KPP objective throughout the program’s life cycle. Achieving improvement targets requires an effective life cycle support model, i.e. a good “Material Availability” KPP strategy. For example, a program’s Material

Availability KPP would necessarily be tightly coupled with that program's NR-KPP improvement targets.

12. The requirement to comply with "commercial best practice for IT" is well documented across the DoD GIG acquisition policy suite. In commercial best IT practice, the concept of KPPs falls under "IT Governance. "

13. In commercial best practice, "IT Governance," is the combination of leadership, repeatable process and metrics that deliver calculable Return on Investment (RoI) to an enterprise via intelligent use of IT.

14. Typical IT governance includes system lead-metrics, (predictors of useful outcomes), system lag-metrics, (measured useful outcomes) and *process metrics* (measures and/or predictors of effective processes).

15. ITIL, CMMI, and Lean Six Sigma are examples of approaches to repeatable process and associated metrics that DoD can apply to IT project governance.

16. "SOA Governance" is the subset of IT governance that addresses intelligent use of service oriented network middleware.

17. The JITC Netcentric Certification Office project has developed a Value-Based Evolutionary Information System Acquisition Framework (VAF) for governing any software-intensive system-of-systems, including SOA. VAF is based on both commercial best practice per paragraphs 15 and 16, and DoD directives per references (a)-(d).

18. The VAF is informed by ITIL, CMMI, and Lean Six Sigma. It has been vetted and iterated with many government and industry experts. Consensus is that the VAF is solid.

19. Per reference (e), (and various GAO reports and countless industrial journals not to mention the Federal Acquisition Regulations (FAR)) "speed-to-capability" is a key requirement for IT acquisition.

20. When it comes to Information Technology (IT), speed to capability is arguably equivalent to, and certainly a predictor of, sustainability.

21. "Speed-to-capability" meets the criteria of a good KPP. That is, speed-to-capability is a predictable and testable lag metric of acquisition process performance necessary to achieve sustainability of modern IT capability.

22. The VAF includes a parameterization of speed-to-capability called "Net-Ready Availability" (A_{nr}). A_{nr} is defined as the initial estimate of development time (T_D) divided by current estimate of Capability Deployment Time (T_{CD}.) T_{CD} is equal to current estimate of Development Time (T_D(c)) plus Test Time (T_T(c)) + Certification Time ((T_c)(c)). The initial estimate of T_{CD} is equal to the threshold or objective speed-to-capability target. If the speed-to-capability target is eighteen months as suggested by per reference (e), and if T_D(i) is twelve months as in a typical large COTS deployment, then A_{nr} = .66. As schedule slips, A_{nr} degrades. As testing and certification are completed in parallel with development, and capabilities are efficiently re-used, A_{nr} improves.

23. A_{nr} can be formulated to identify variables that can be adjusted to achieve its objective and threshold values. For example, $T_D(c)$ might be equal to Invention Time (T_I) + Reinvention Time (T_R) + Bundling Time (T_B) + Overhead Time (T_O). Programs should reserve Invention Time only to develop capabilities not available off-the-shelf. They should design "Invented" capabilities for subsequent ease of re-use. Programs should generally avoid Re-invention Time. Bundling Time is the time it takes to combine components to interact usefully. Programs can define T_B in terms of Build Time, and/or Run Time. Achieving target values of BT typically requires careful choice of standards and implementation methods.

24. The VAF includes a parameterization called "Information Value Availability" (A_{iv}.) A_{iv} is conceptually equal to "Valued Bits" (VB) divided by "Total Bits Processed" (TB). This parameterization recognizes the information overload issue. It aims to help system designers reserve human processing time for the most critical tasks. VAF identifies Valued Bits by analyzing critical mission thread transactions in context with user-defined operational effectiveness targets. Generally, actionable bits are more valued than all others. VAF applies this operational analysis to define the technical information exchange requirements -- such as for "tagging", "registering", "discovery," "smart push", "smart pull" etc -- necessary to achieve targeted operational performance outcomes.

25. Per reference (d) abbreviated interpretation of the "Pillars of the NR-KPP" follows:

a. **Supportability**: Assure connectivity to electromagnetic spectrum as necessary to create a distributed military computer network. Supportability pillar emphasizes compliance with Joint Tactical Radio System (JTRS). (Inexplicably and unlike references (a)-(c), reference (d) does not address "supportability" beyond the narrow confines of spectrum issues. For example, a very expensive, bulky, heavy, power-constrained, all-purpose, radio that is proprietary to a single vendor, might satisfy this pillar. However, such a radio would certainly not be "supportable" in any practical sense.)

b. **Data and services strategy**: Assure availability of useful information.

c. **Information Assurance:** Assure non-repudiation, integrity, confidentiality, authentication, and *information availability*.

d. **GIG technical guidance**: Translate DoD IT acquisition IT policy imperatives such as "commercial best practice," "open modular design,""re-use,""risk adaptive access control," "need-to-share vice need-to-know," and "rapid, iterative, development," into an engineering framework optimized to deliver value to the DoD GIG enterprise.

e. **Compliant solution architecture**: Provide the design constraints necessary to achieve all the above.

26. The VAF provides a formulation (Ai_v) of the NR-KPP that is consistent with commercial best practice. Further, VAF tightly couples the NR-KPP to the Material Availability KPP via A_{nr}. VAF generally addresses the pillars of the NR-KPP as follows:

a. **Supportability**: The VAF constrains JTRS/spectrum-compliant solutions to practical form factors and life cycle support models. Speed-to-capability is effectively equivalent to non-spectrum aspects of "supportability" for IT systems as it is defined in references (a)-(c). VAF requires candidate radio solutions to demonstrate credible speed-to-capability models throughout their life cycles. (For example, DoD might furnish JTRS wave forms and NCES security services as “Government Furnished Equipment” (GFE). Vendors could then bundle military software-defined radios in cell phone form factors. Cell phone applications (e.g. iPhone Apps) might include military-specific capability along with generic capability.)

b. **Data and services strategy**: Aiv is designed as an NR-KPP for a software-intensive system-of-systems. It tightly couples desired mission outcomes to technical exchange requirements in a testable way. The VAF helps programs manage data, standards, schemas, and information exchanges to improve iteratively from threshold to objective values of NR-KPP. (We know that specifying specific standards a priori is a failed strategy for building large software-intensive systems. Hence, the NR-KPP process should include useful guidance to help programs select appropriate standards and implementation, in context with commercial state-of-the art, and based on their specific NR-KPP formulation. This means that NR-KPP certifiers should become joined at the hip with the standards bodies and best-practice centers of excellence.)

c. **Information assurance:** VAF “builds in” security from the ground up per NSA GIG IA policy. VAF reduces non-repudiation, integrity, confidentiality, and authentication into verifiable attributes. VAF also objectively address the need-to-share vs. need-to-know trade off issue per the “Information Availability” component of IA.

d. **GIG technical guidance**: VAF is an IT project governance model based on industrial best practice and specifically constructed to enable GIG “business objectives” -- i.e. rapid, cost effective acquisition to enable operational information superiority -- through IT paradigms like SOA, “Cloud”, and Open Technology Development.

e. **Compliant solutions architecture**: Architectural artifacts should be the byproduct of design. However, many practitioners employ DoDAF merely to create architectural documentation that complies with policy for architectural documentation. A case in point is that the Joint C2 Architecture and Capability Assessment Enterprise (JACAE) tool does not link IT standards to system or mission performance. By contrast, the VAF provides design tools that connect to objectively defined performance outcomes. By adding VAF to the JACAE and similar tools, we can automate an NR-KPP-compliant solutions architecture design process.

C.R. Gunderson